



State of Indiana Cyber Security



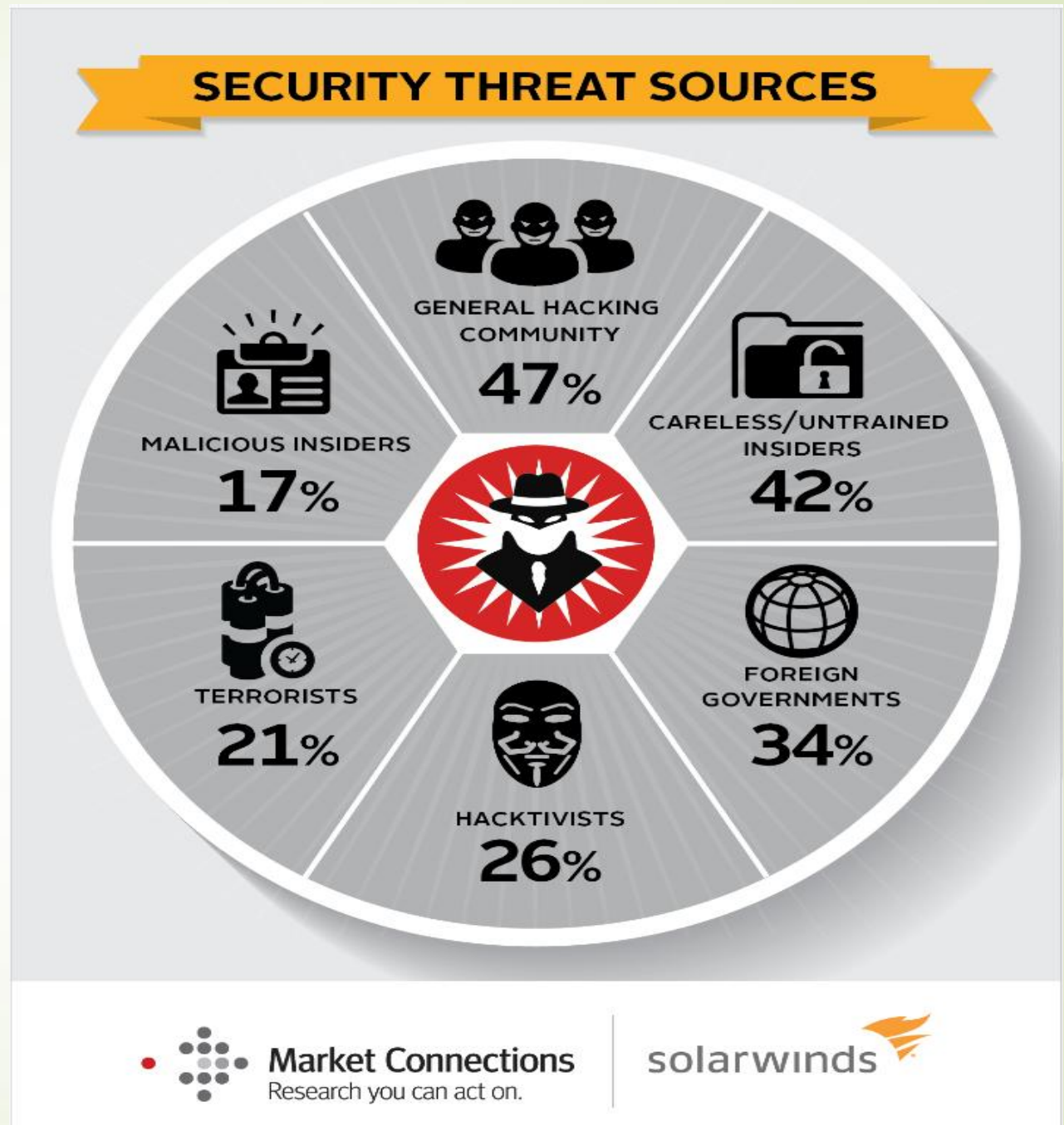
Some background

- State of Indiana, Executive Branch
- 30,000+ workers
- 800+ systems
- 100+ agencies
- Millions of records containing personally identifiable information (PII)

Cyber Threats



Threat Sources



Target: Personal Information



Target: Loss of Public Trust





Our Protective Strategy



- Evaluate the threat
- Consider the damage and the likelihood
- Prioritize
- Mitigate

Threats

External hacking

Malware

Social engineering

Spam

**Insider data leakage,
theft**

Denial of service

Mobile device theft

**Physical security
attacks**

Continuing the Analysis

- Less concerned about the who or why – rarely anything we can do
- More on our ability to fend off regardless – must have a program
- Some you see daily, others you see coming
- Insider threats, both accidental and malicious have been elevated in our priorities

Threats	Threat Sources
External hacking	Hackers, foreign governments, hactivists
Malware	Hackers, foreign governments, hactivists
Social engineering	Hackers, foreign governments, hactivists
Spam	Hackers, foreign governments, hactivists
Insider data leakage, theft	Careless, untrained insiders, malicious insiders
Denial of service	Hackers, foreign governments, hactivists
Mobile device theft	Careless, untrained insiders, malicious insiders
Physical security attacks	Terrorists

Determining risk levels and priorities

- These three factors, along with the environment can identify likelihood
- The likelihood and potential damage drive our priorities, our defensive decisions

Threats	Threat Sources	Targets
External hacking	Hackers, foreign governments, hactivists	Personal information, public trust
Malware	Hackers, foreign governments, hactivists	Personal information
Social engineering	Hackers, foreign governments, hactivists	Personal information
Spam	Hackers, foreign governments, hactivists	Personal information
Insider data leakage, theft	Careless, untrained insiders, malicious insiders	Personal information
Denial of service	Hackers, foreign governments, hactivists	Public trust
Mobile device theft	Careless, untrained insiders, malicious insiders	Personal information
Physical security attacks	Terrorists	Public trust

Protections

Threats	Sources	Targets	Protections - layers
External hacking	Hackers, foreign governments, hactivists	Personal information, public trust	Firewall, web application firewall, Server AV, SIEM, Solid Core, least privilege, policy, secure code, pen testing
Malware	Hackers, foreign governments, hactivists	Personal information	Email gateway – 2, Server and workstation AV, network signature detection, Internet filter, IDS, training and awareness
Social engineering	Hackers, foreign governments, hactivists	Personal information	Internet filter, Email gateways, policies, training and awareness
Spam	Hackers, foreign governments, hactivists	Personal information	Email gateways, Server and workstation AV, network signature detection, Internet filter, training and awareness
Insider data leakage, theft	Careless, untrained insiders, malicious insiders	Personal information	Application logs, host IDS, database auditing, SIEM, NIST
Denial of service	Hackers, foreign governments, hactivists	Public trust	IN.gov
Mobile device theft	Careless, untrained insiders, malicious insiders	Personal information	Encryption – laptops, flash drives, MobileIron
Physical security attacks	Terrorists	Public trust	Captiol Police, data center physical protection



Questions

- ▶ Tad Stahl, CISO
Indiana Office of Technology

tstahl@iot.in.gov

234-3434

